BRUNNER QUINN

PARTNERS
Rick L. Brunner * ◊ °
Patrick M. Quinn~

ASSOCIATES
Peter A. Contreras †
Kaitlin L. Madigan

OF COUNSEL
Steven M. Brown

* Also admitted in PA
† Also admitted in FL
◊ Also admitted in DC
° Also admitted in NY
~ Also admitted in WV

Rick L. Brunner
35 North Fourth Street
Suite 200
Columbus, Ohio 43215
(614) 241-5550, Ext. 226
(800) 776-3158, Toll-Free
(614) 241-5551, Fax
rlb@brunnerlaw.com

January 9, 2015

Via Certified U.S. & Electronic Mail & Facsimile
Detective Jeremy Dye
Hocking County Sheriff's Office
25 East Second Street
Logan, OH 43138
Facsimile: 740-380-2121
Email: sheriff@co.hocking.oh.us
Email: sheriff@hockingsheriff.org,

RE: (i) *preservation of all electronic records and communications related to or concerning David Cummin MD, Hocking County Coroner or the Hocking County Coroner's office in any way whatsoever and/or it's or the coroner's interaction with any other County office holder or their staff*;
(ii) *David Cummin, et al . vs. Laina Fetherolf a.k.a. Laina Fetherolf Rogers, a.k.a. Laina Rose Rogers, , et al.,* United States District Court for the Southern District of Ohio Proposed litigation

Detective Jeremy Dye:

This office has been retained to represent David Cummin M.D. regarding the above-referenced matters.

While we remain hopeful that the proposed Defendants will now engage in meaningful discussion of resolution, with regards to both matters we are very concerned about the destruction of electronic communications and other electronically stored information between you or your office and all the other parties to these communications including communications on which you or someone in your office have been copied including but not limited to William L "Bill" Archer, Laina Fetherolf, L. Rose Rogers, C. David Warren, James K. Stanley, Esq., former Commissioner, John Walker, or any Hocking County Commissioner or staff, Chief Deputy David Valkinburg, Detective Edwin Downs, Captain Jarod Alford, former Sherriff Lanny North, Detective Caleb Moritz, BCI&I. Chief Steve Schierholt and Buckeye Sheriff Association, County Commissioners Association, and Prosecutors Association, or any of these individuals or firms' agents and representatives and the preservation of the same. To that end, we issue the following caution:

EXHIBIT
tabbies
6

1. Preservation of Evidence

NOTICE TO PRINCIPALS IS NOTICE TO AGENTS. NOTICE TO AGENTS IS NOTICE TO PRINCIPALS.

DEMAND FOR PRESERVATION OF ELECTRONICALLY STORED INFORMATION

By this notice we hereby demand that you preserve all documents, tangible things and electronically stored information ("ESI") potentially relevant to communications with and/or about any of the above referenced matters of litigation. As used in this document, "you" and "your" refers to you or anyone at your office or agency, and your office's or agency's or firm's predecessors, successors, parents, subsidiaries, divisions or affiliates, and their respective officers, directors, agents, attorneys, accountants, employees, partners or other persons occupying similar positions or performing similar functions or staff of the same.

You should anticipate that much of the information subject to disclosure or responsive to discovery in this matter is stored on your current and former computer systems and other media and devices (including personal digital assistants, voice-messaging systems, online repositories and cell phones).

Electronically stored information (hereinafter "ESI") should be afforded the broadest possible definition and includes (by way of example and not as an exclusive list) potentially relevant information electronically, magnetically or optically stored as:

- Digital communications (e.g., e-mail, voice mail, instant messaging);
- Word processed documents (e.g., Word or WordPerfect documents and drafts);
- Spreadsheets and tables (e.g., Excel or Lotus 123 worksheets);
- Accounting Application Data (e.g., QuickBooks, Money, Peachtree data files);
- Image and Facsimile Files (e.g., .PDF, .TIFF, .JPG, .GIF images);
- Sound Recordings (e.g., .WAV and .MP3 files);
- Video and Animation (e.g., .AVI and .MOV files);
- Databases (e.g., Access, Oracle, SQL Server data, SAP, etc.);
- Contact and Relationship Management Data (e.g., Outlook, ACT!);
- Calendar and Diary Application Data (e.g., Outlook PST, Gmail, Lotus Notes, Yahoo, blog tools);
- Online Access Data (e.g., Temporary Internet Files, History, Cookies);
- Presentations (e.g., PowerPoint, Corel Presentations)
- Network Access and Server Activity Logs;
- Project Management Application Data;
- Computer Aided Design/Drawing Files; and,
- Back Up and Archival Files (e.g., tapes, Zip, .TAR, .GHO)

ESI resides not only in areas of electronic, magnetic and optical storage media reasonably accessible to you, but also in areas you may deem *not* reasonably accessible. You are obliged to *preserve* potentially relevant evidence from *both* these sources of ESI, even if you do not anticipate *producing* such ESI. The demand that you preserve both accessible and inaccessible ESI is reasonable and necessary. Pursuant to amendments to the Federal Rules of Civil Procedure that have been approved by the United States Supreme Court (eff. 12/1/06), you must identify all sources of ESI you decline to produce and demonstrate to the court why such sources are not reasonably accessible. For good cause shown, the court

may then order production of the ESI, even if it finds that it is not reasonably accessible. Accordingly, even ESI that you deem reasonably inaccessible *must be preserved in the interim* so as not to deprive my clients of their right to secure the evidence or the Court of its right to adjudicate the issue.

PRESERVATION REQUIRES IMMEDIATE INTERVENTION

You must act immediately to preserve potentially relevant ESI including January 1, 2012 through the date of this demand with an ongoing duty to preserve future relevant communication.

Adequate preservation of ESI requires more than simply refraining from efforts to destroy or dispose of such evidence. You must also intervene to prevent loss due to routine operations and employ proper techniques and protocols suited to protection of ESI. *Be advised that sources of ESI are altered and erased by continued use of your computers and other devices.* Booting a drive, examining its contents or running any application will irretrievably alter the evidence it contains and may constitute unlawful spoliation of evidence. Consequently, alteration and erasure may result from your failure to act diligently and responsibly to prevent loss or corruption of ESI. *Nothing in this demand for preservation of ESI should be understood to diminish your concurrent obligation to preserve documents, tangible things and other potentially relevant evidence.*

SUSPENSION OF ROUTINE DESTRUCTION

You are directed to immediately initiate a litigation hold for potentially relevant ESI, documents and tangible things, and to act diligently and in good faith to secure and audit compliance with such litigation hold. You are further directed to immediately identify and modify or suspend features of your information systems and devices that, in routine operation, operate to cause the loss of potentially relevant ESI. Examples of such features and operations include:

- Purging the contents of e-mail repositories by age, capacity or other criteria;
- Using data or media wiping, disposal, erasure or encryption utilities or devices;
- Overwriting, erasing, destroying or discarding back up media;
- Re-assigning, re-imaging or disposing of systems, servers, devices or media;
- Running antivirus or other programs effecting wholesale metadata alteration;
- Releasing or purging online storage repositories;
- Using metadata stripper utilities;
- Disabling server or IM logging; and,
- Executing drive or file defragmentation or compression programs.

GUARD AGAINST DELETION

You should anticipate that your employees, officers or others may seek to hide, destroy or alter ESI and act to prevent or guard against such actions. Especially where company machines have been used for Internet access or personal communications, you should anticipate that users may seek to delete or destroy information they regard as personal, confidential or embarrassing and, in so doing, may also delete or destroy potentially relevant ESI. This concern is not one unique to you or your employees and officers.

It's simply an event that occurs with such regularity in electronic discovery efforts that any custodian of ESI and their counsel are obliged to anticipate and guard against its occurrence.

PRESERVATION BY IMAGING

You should take affirmative steps to prevent anyone with access to your data, systems and archives from seeking to modify, destroy or hide electronic evidence on network or local hard drives (such as by deleting or overwriting files, using data shredding and overwriting applications, defragmentation, re-imaging or replacing drives, encryption, compression, steganography or the like). With respect to local hard drives, one way to protect existing data on local hard drives is by the creation and authentication of a forensically qualified image of all sectors of the drive. Such a forensically qualified duplicate may also be called a bitstream image or clone of the drive. Be advised that a conventional back up of a hard drive is not a forensically qualified image because it only captures active, unlocked data files and fails to preserve forensically significant data that may exist in such areas as unallocated space, slack space and the swap file.

With respect to the hard drives and storage devices of each person likely to have information pertaining to the instant action on their computer hard drive(s), demand is made that you immediately obtain, authenticate and preserve forensically qualified images of the hard drives in any computer system (including portable and home computers) used by that person during the period from January 1, 2012 to present date, as well as recording and preserving the system time and date of each such computer. Once obtained, each such forensically qualified image should be labeled to identify the date of acquisition, the person or entity acquiring the image and the system and medium from which it was obtained. Each such image should be preserved without alteration.

PRESERVATION IN NATIVE FORM

You should anticipate that certain ESI, including but not limited to spreadsheets and databases, will be sought in the form or forms in which it is ordinarily maintained. Accordingly, you should preserve ESI in such native forms, and you should not select methods to preserve ESI that remove or degrade the ability to search your ESI by electronic means or make it difficult or burdensome to access or use the information efficiently in the litigation. You should additionally refrain from actions that shift ESI from reasonably accessible media and forms to less accessible media and forms if the effect of such actions is to make such ESI not reasonably accessible.

METADATA

You should further anticipate the need to disclose and produce system and application metadata and act to preserve it. System metadata is information describing the history and characteristics of other ESI. This information is typically associated with tracking or managing an electronic file and often includes data reflecting a file's name, size, custodian, location and dates of creation and last modification or access. Application metadata is information automatically included or embedded in electronic files but which may not be apparent to a user, including deleted content, draft language, commentary, collaboration and distribution data and dates of creation and printing. Be advised that metadata may be overwritten or corrupted by careless handling or improper steps to preserve ESI. For electronic mail, metadata includes

all header routing data and Base 64 encoded attachment data, in addition to the To, From, Subject, Received Date, CC and BCC fields.

SERVERS

With respect to servers like those used to manage electronic mail (e.g., Microsoft Exchange, Lotus Domino) or network storage (often called a user's "network share"), the complete contents of each user's network share and e-mail account should be preserved. There are several ways to preserve the contents of a server depending upon, e.g., its RAID configuration and whether it can be downed or must be online 24/7. If you question whether the preservation method you pursue is one that we will accept as sufficient, please call to discuss it.

HOME SYSTEMS, LAPTOPS, ONLINE ACCOUNTS AND OTHER ESI VENUES

Though we expect that you will act swiftly to preserve data on office workstations and servers, you should also determine if any home or portable systems may contain potentially relevant data. To the extent that officers, board members or employees have sent or received potentially relevant e-mails or created or reviewed potentially relevant documents away from the office, you must preserve the contents of systems, devices and media used for these purposes (including not only potentially relevant data from portable and home computers, but also from portable thumb drives, CD-R disks and the user's PDA, smart phone, voice mailbox or other forms of ESI storage). Similarly, if employees, officers or board members used online or browser-based email accounts or services (such as AOL, Gmail, Yahoo Mail or the like) to send or receive potentially relevant messages and attachments, the contents of these account mailboxes (including Sent, Deleted and Archived Message folders) should be preserved.

ANCILLARY PRESERVATION

You must preserve documents and other tangible items that may be required to access, interpret or search potentially relevant ESI, including logs, control sheets, specifications, indices, naming protocols, file lists, network diagrams, flow charts, instruction sheets, data entry forms, abbreviation keys, user ID and password rosters or the like. You must preserve any passwords, keys or other authenticators required to access encrypted files or run applications, along with the installation disks, user manuals and license keys for applications required to access the ESI. You must preserve any cabling, drivers and hardware, other than a standard 3.5" floppy disk drive or standard CD or DVD optical disk drive, if needed to access or interpret media on which ESI is stored. This includes tape drives, bar code readers, Zip drives and other legacy or proprietary devices.

PAPER PRESERVATION OF ESI IS INADEQUATE

As hard copies do not preserve electronic searchability or metadata, they are not an adequate substitute for, or cumulative of, electronically stored versions. If information exists in both electronic and paper forms, you should preserve both forms.

AGENTS, ATTORNEYS AND THIRD PARTIES

Your preservation obligation extends beyond ESI in your care, possession or custody and includes ESI in the custody of others that is subject to your direction or control. Accordingly, you must notify any current or former agent, attorney, employee, custodian or contractor in possession of potentially relevant ESI to preserve such ESI to the full extent of your obligation to do so, and you must take reasonable steps to secure their compliance.

PRESERVATION PROTOCOLS

We are desirous of working with you to agree upon an acceptable protocol for forensically sound preservation and can supply a suitable protocol, if you will furnish an inventory of the systems and media to be preserved. Also, if you will promptly disclose the preservation protocol you intend to employ, perhaps we can identify any points of disagreement and resolve them. A successful and compliant ESI preservation effort requires expertise. If you do not currently have such expertise at your disposal, we urge you to engage the services of an expert in electronic evidence and computer forensics. Perhaps our respective experts can work cooperatively to secure a balance between evidence preservation and burden that's fair to both sides and acceptable to the Court.

DO NOT DELAY PRESERVATION

I'm available to discuss reasonable preservation steps; however, *you should not defer preservation steps pending such discussions if ESI may be lost or corrupted as a consequence of delay.* Should your failure to preserve potentially relevant evidence result in the corruption, loss or delay in production of evidence to which we are entitled, such failure would constitute spoliation of evidence, and we will not hesitate to seek sanctions.

CONFIRMATION OF COMPLIANCE

Please confirm by January 23, 2015 that you have taken the steps outlined in this letter to preserve ESI and tangible documents potentially relevant to this action. If you have not undertaken the steps outlined above, or have taken other actions, please describe what you have done to preserve potentially relevant evidence.

In conclusion, all communication regarding this matter should be directed through this office. Should you have any questions or concerns, please do not hesitate to contact this office.

Your prompt attention to this matter is required to avoid the cost and inconvenience of immediate multi-state and multi-jurisdictional legal and administrative action.

Very Truly Yours,

Rick L. Brunner, Esq.

RLB/jab

cc: client

Patrick M Quinn, Esq.
Peter A Contreras, Esq.
Kaitlin L Madigan, Esq.